m.it.s co

Morvarid. IT. Solutions Co.

MikroTik

MUM - Manila, Philippines - April 13th 2016

Dude Server

iGenTik

By

Mani Raissdana

Mani Raissdana

MikroTik Certified Trainer
Ubiquiti Certified Trainer
elastiX Certified Trainer
m.it.s co. CTO & Co. Founder
Morvarid. IT. Solutions Co.

Philippines Partner: DOUBLESQUARE NETWORKS INC.

Being in IT technology business roughly around 14 years

Support & instruct Engineers more than 8 years all over the globe

Wireless, Routing, QoS, Firewall, The Dude

Mani Raissdana

- **MikroTik Certified Trainers**

http://www.mikrotik.com/training/partners/europe/turkey

- **MikroTik Certified Consultants**

http://www.mikrotik.com/consultants/europe/turkey

- **Mani Raissdana Certifications**

http://www.mikrotik.com/certificateSearch Check Mani Raissdana

http://www.mits-co.com/content/certificates

- **Ubiquiti Certified Trainers**

https://www.ubnt.com/training/partners/ Check Europe

- **elastiX Certified Trainers**

http://www.elastix.com/en/instructores/ Check Turkey

- **elastiX Official Resellers**

http://www.elastix.com/en/resellers-elastix/ Check Europe

- **Mani Raissdana Resume**

www.mits-co.com/sites/default/files/Mani%20Raissdana%20Resume.pdf

MikroTik
MikroTik
DOUBLESQUARE
MikroTik

Training Schedule

http://www.mikrotik.com/training/	Check M.IT.S Co
https://www.ubnt.com/training/calendar/	Check M.IT.S Co
http://www.elastix.com/en/events-3/	Check M.IT.S Co

http://www.mits-co.com/training_mikrotik%20

http://www.mits-co.com/training_ubiquiti

http://www.mits-co.com/training_elastix

GALLERY

MITS & MICROTIK

Manila upcoming training sessions

April 14-16

MikroTik MTCNA

April 17-18

MikroTik MTCRE

April 19-20

MikroTik MTCINE

April 21-22

MikroTik MTCTCE

April 23-24

MikroTik MTCWE

April 25-26

MikroTik MTCUME

April 26-30 (Elastix/ Asterisk)

elastix CERTIFIED ENGINEER

Table of contents

Dude

- What is Dude???
- What it does???
- How it works???
- How you should work with???
- Monitoring
- Notification

iGenTik

Interactive GSM/Email notification system

WS
FORUM
SOCIAL NETWORK
CONTENT SHARING
MICROBLOGS
SOCIAL MEDIA
VIDEO
COMMUNICATION
CHAT
PICTURE
OUR BUSINESS
OK
EA
OTHER
COMPETITOR
OUR COMPANY
YES
?
35%
$
TIME
MONE
BUSINESS
QUALITY
ROUTER
AUTHENTICATION SERVER
CLIENT 1
CLIENT 2
CLIENT n.
1010001
1010100
FIREWALL
SERVER F
INTERNET
VOIP
COMPANY HEADQUARTERS
GROWTH
+61
SEARCH ENGINE
DESIGN
MEDIA
SMS
STATISTICS
$
500.000
LAST YEAR
$
1.000.
THIS Y
QUALITY
STRATEGY
VISI
SUCCESS
INNOVATION
VISI
RESEARCH
BLOG
0%
150%
SOCIAL NETWORK

What is Dude

- MikroTik free Monitoring application
- Has 2 parts:

1. Client application: (Windows, Mac, Linux)
2. Server package: (RoS package) only for:

- MikroTik CCR Series
- RouterOS X86
- RouterOS CHR

RouterOS Version should be 6.34rc13 or higher to be able to use Dude

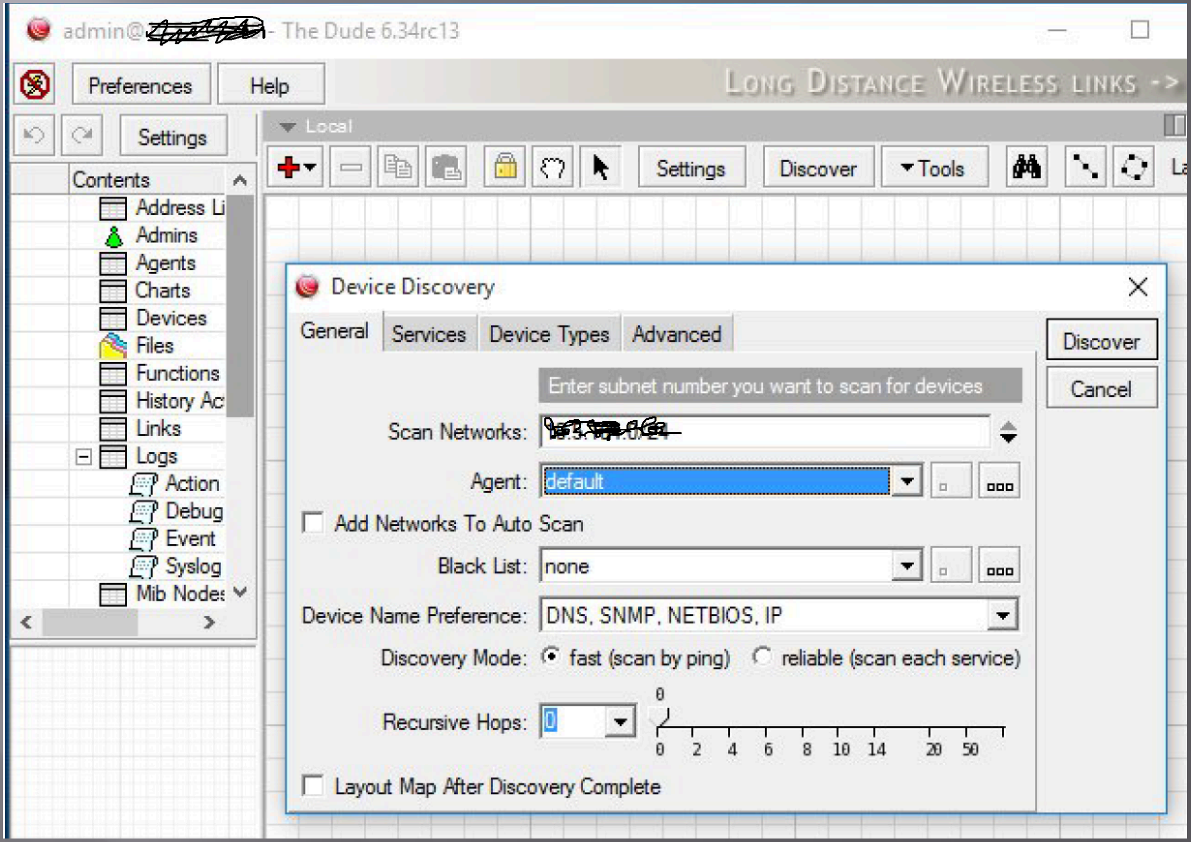
What it Does

- Scans (Discovers) your Network in layer 2
- Monitors availability of your network
- Keeps watching all your layer 3 devices
- Monitors all your links
- Supports layer 3 probes
- Supports SNMP
- Has direct access to your RouterOS (with Winbox)

Here, we're talking about Dude V6, Which has some fundamental differences with legacy versions

How it works

- After successful Installation, login page comes up
- After Successful Login, Automatic Discovery feature will jump up,



admin@[redacted] - The Dude 6.34rc13

Device Discovery

Enter subnet number you want to scan for devices

Scan Networks: [redacted]

Agent: default

□ Add Networks To Auto Scan

Black List: none

Device Name Preference: DNS, SNMP, NETBIOS, IP

Discovery Mode: ● fast (scan by ping) ○ reliable (scan each service)

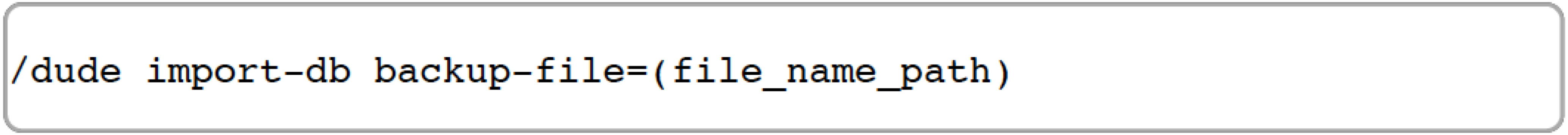
Recursive Hops: 0

□ Layout Map After Discovery Complete

- You may like to discover your Network automatically or add everything manually

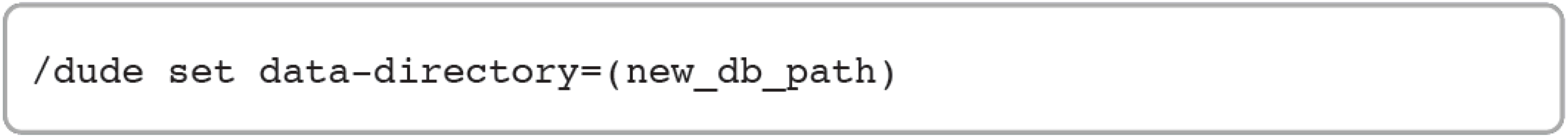
How it works

- If you are working with legacy versions (V3 or V4), you are still be able to import your old database here



```
/dude import-db backup-file=(file_name_path)
```

- Or maybe you'd like to change the path of database



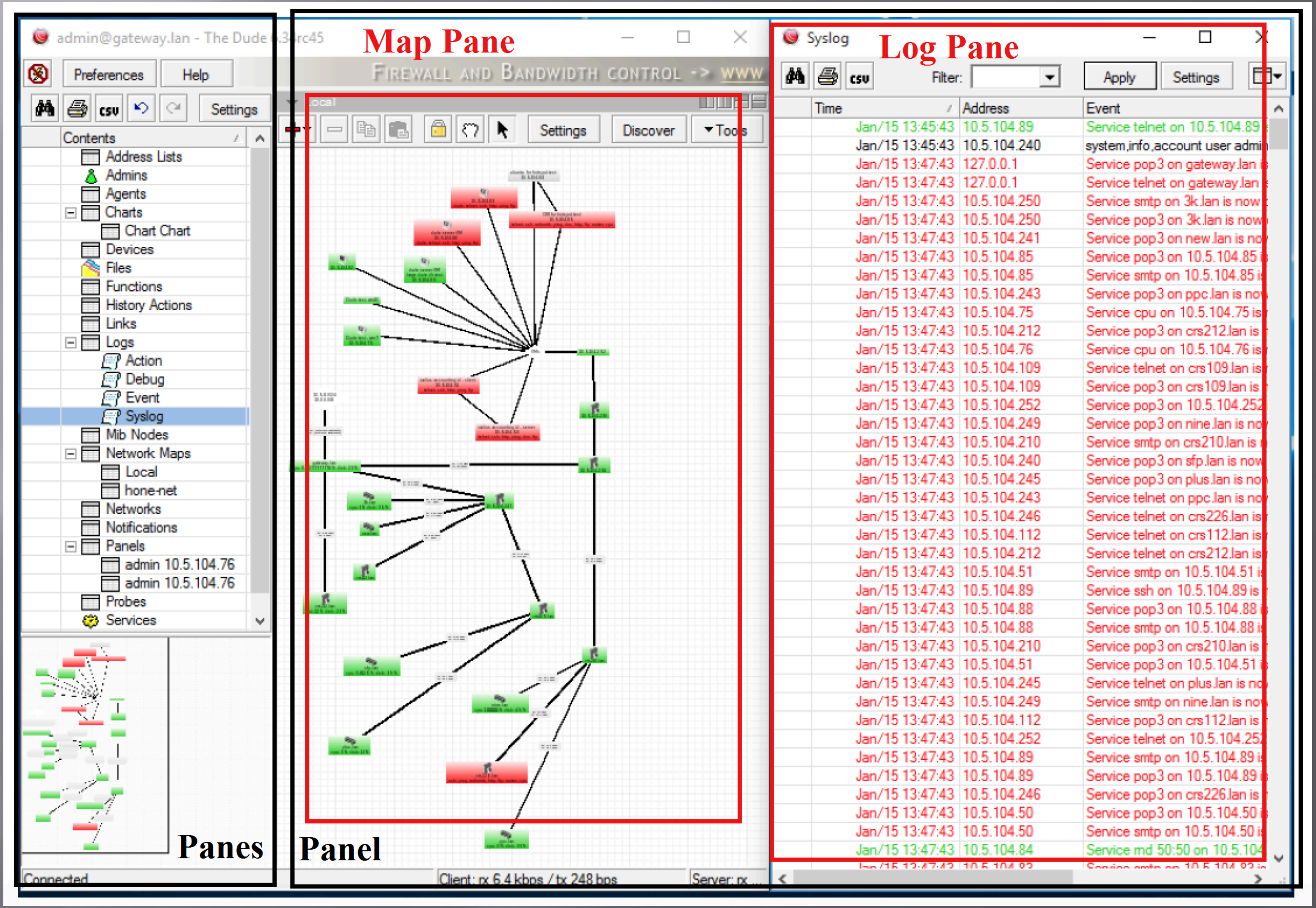
```
/dude set data-directory=(new_db_path)
```

Change path procedure:

1. Disable the Server
2. Move existing directory
3. Change the path of directory
4. Enable the Server

How you should work with

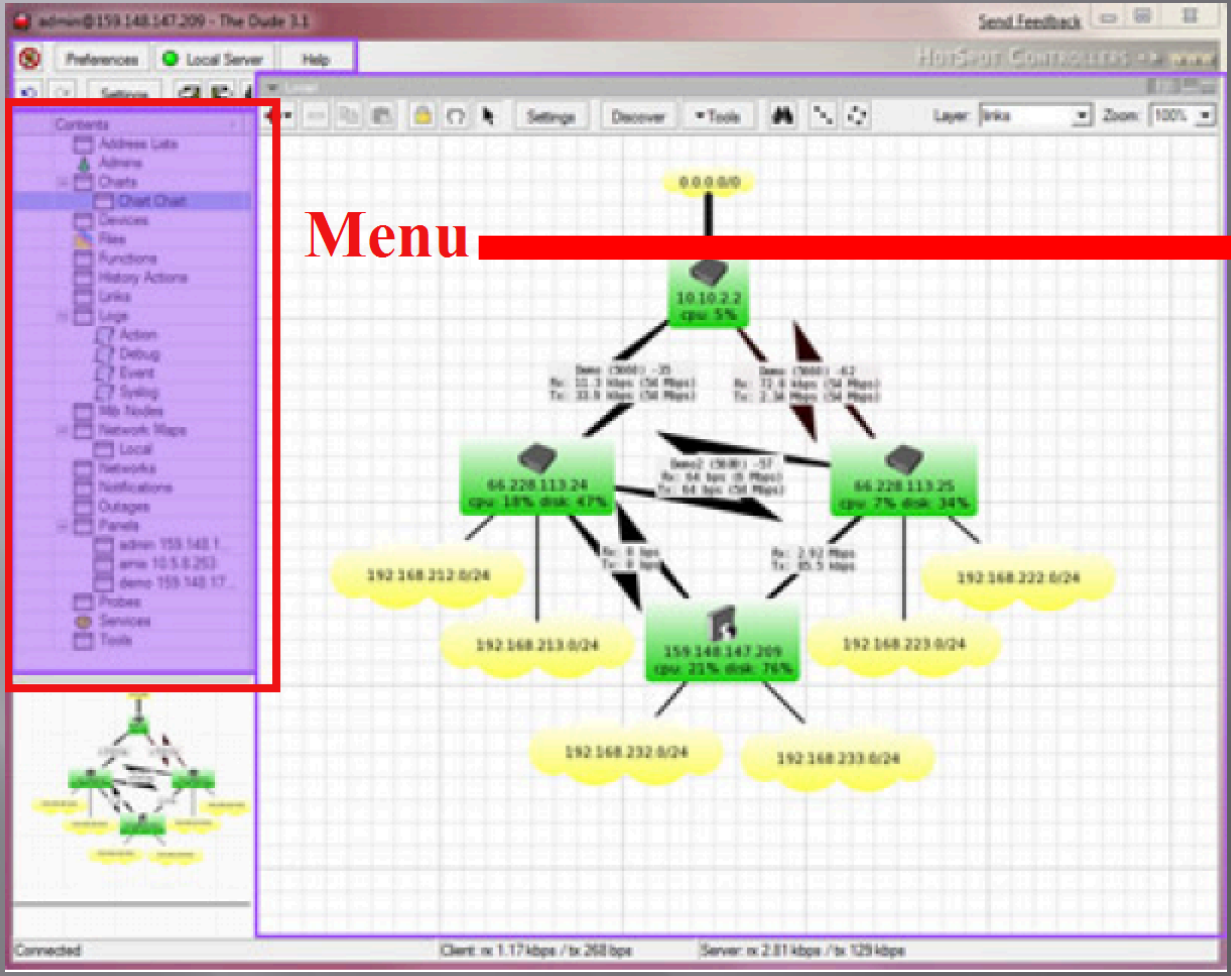
Interface



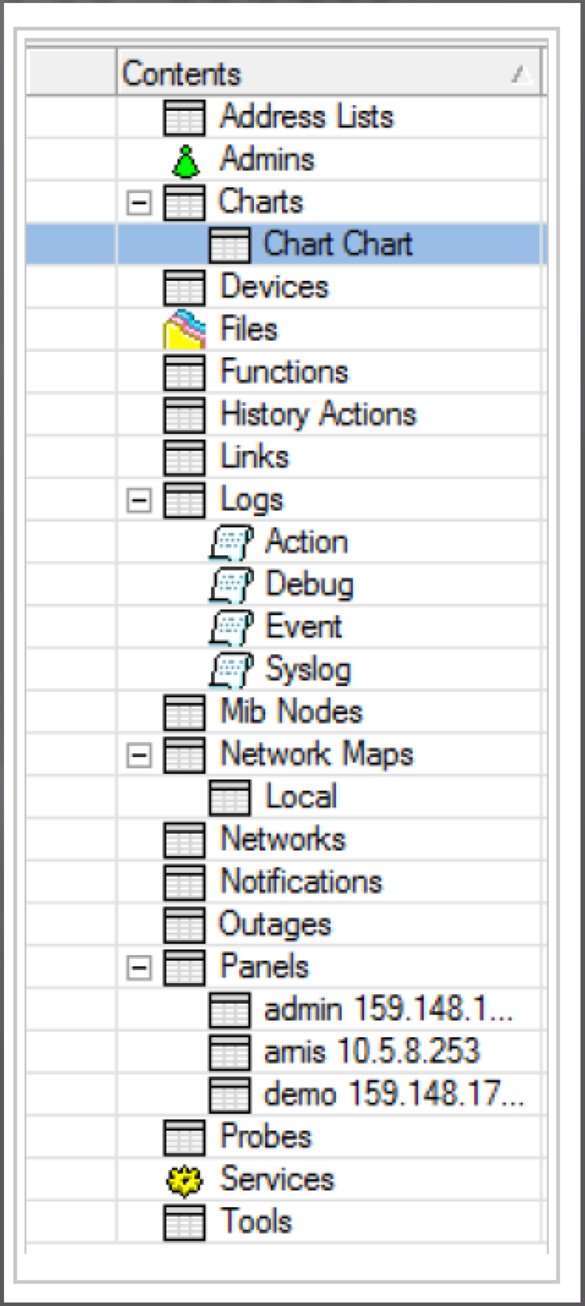
```
Time              Address        Event
Jan/15 13:45:43   10.5.104.89    Service telnet on 10.5.104.89
Jan/15 13:45:43   10.5.104.240   system,info,account user admi
Jan/15 13:47:43   127.0.0.1      Service pop3 on gateway.lan i
Jan/15 13:47:43   127.0.0.1      Service telnet on gateway.lan
Jan/15 13:47:43   10.5.104.250   Service smtp on 3k.lan is now
Jan/15 13:47:43   10.5.104.250   Service pop3 on 3k.lan is now
Jan/15 13:47:43   10.5.104.241   Service pop3 on new.lan is no
Jan/15 13:47:43   10.5.104.85    Service pop3 on 10.5.104.85 i
Jan/15 13:47:43   10.5.104.85    Service smtp on 10.5.104.85 is
Jan/15 13:47:43   10.5.104.243   Service pop3 on ppc.lan is no
Jan/15 13:47:43   10.5.104.75    Service cpu on 10.5.104.75 is
Jan/15 13:47:43   10.5.104.212   Service pop3 on crs212.lan is
Jan/15 13:47:43   10.5.104.76    Service cpu on 10.5.104.76 is
Jan/15 13:47:43   10.5.104.109   Service telnet on crs109.lan is
Jan/15 13:47:43   10.5.104.109   Service pop3 on crs109.lan is
Jan/15 13:47:43   10.5.104.252   Service pop3 on 10.5.104.252
Jan/15 13:47:43   10.5.104.249   Service pop3 on nine.lan is no
Jan/15 13:47:43   10.5.104.210   Service smtp on crs210.lan is
Jan/15 13:47:43   10.5.104.240   Service pop3 on sfp.lan is now
Jan/15 13:47:43   10.5.104.245   Service pop3 on plus.lan is no
Jan/15 13:47:43   10.5.104.243   Service telnet on ppc.lan is no
Jan/15 13:47:43   10.5.104.246   Service telnet on crs226.lan is
Jan/15 13:47:43   10.5.104.112   Service telnet on crs112.lan is
Jan/15 13:47:43   10.5.104.212   Service telnet on crs212.lan is
Jan/15 13:47:43   10.5.104.51    Service smtp on 10.5.104.51 is
Jan/15 13:47:43   10.5.104.89    Service ssh on 10.5.104.89 is
Jan/15 13:47:43   10.5.104.88    Service pop3 on 10.5.104.88 i
Jan/15 13:47:43   10.5.104.88    Service smtp on 10.5.104.88 is
Jan/15 13:47:43   10.5.104.210   Service pop3 on crs210.lan is
Jan/15 13:47:43   10.5.104.51    Service pop3 on 10.5.104.51 i
Jan/15 13:47:43   10.5.104.245   Service telnet on plus.lan is no
Jan/15 13:47:43   10.5.104.249   Service smtp on nine.lan is no
Jan/15 13:47:43   10.5.104.112   Service pop3 on crs112.lan is
Jan/15 13:47:43   10.5.104.252   Service telnet on 10.5.104.25
Jan/15 13:47:43   10.5.104.89    Service smtp on 10.5.104.89 is
Jan/15 13:47:43   10.5.104.89    Service pop3 on 10.5.104.89 i
Jan/15 13:47:43   10.5.104.246   Service pop3 on crs226.lan is
Jan/15 13:47:43   10.5.104.50    Service pop3 on 10.5.104.50 i
Jan/15 13:47:43   10.5.104.50    Service smtp on 10.5.104.50 is
Jan/15 13:47:43   10.5.104.84    Service md 50:50 on 10.5.104
Jan/15 13:47:43   10.5.104.82    Service smtp on 10.5.104.82 is
```

How you should work with

Menu



Menu



Contents

- Address Lists
- Admins
- Charts
  - Chart Chart
- Devices
- Files
- Functions
- History Actions
- Links
- Logs
  - Action
  - Debug
  - Event
  - Syslog
- Mib Nodes
- Network Maps
  - Local
- Networks
- Notifications
- Outages
- Panels
  - admin 159.148.1...
  - amis 10.5.8.253
  - demo 159.148.17...
- Probes
- Services
- Tools

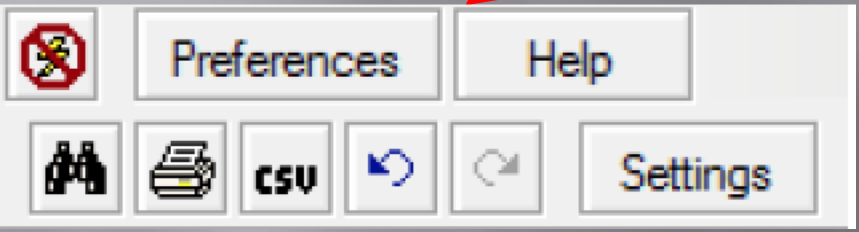
How you should work with

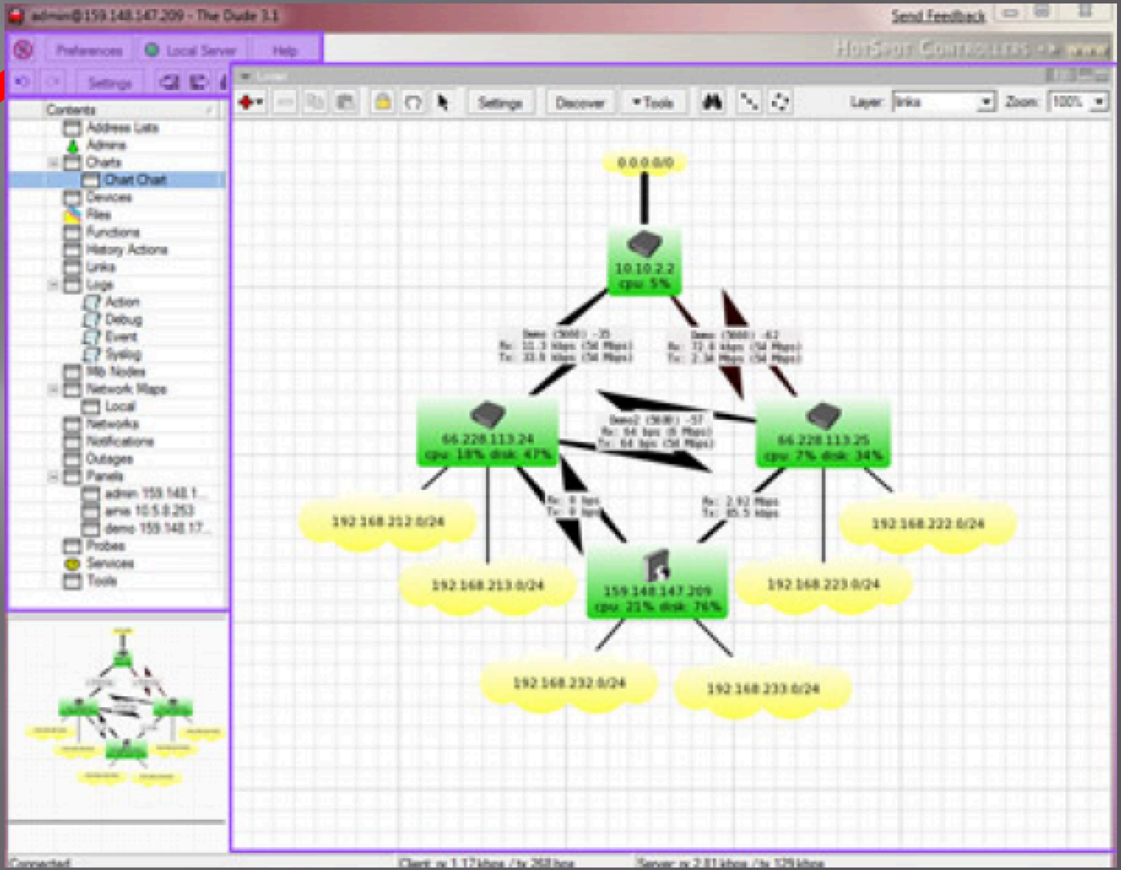
Menu

- Address lists: Lists of IP addresses to be used in Blocklist and other places
- Admins: Users who can access this particular Dude server
- Charts: Configure graphs based on any data source in the map
- Devices: List of all the devices drawn on any of the network maps
- Files: List of the files uploaded to the server, like images for network map backgrounds and sounds
- Functions: Functions that can be used, includes scripts and advanced queries
- History Actions: History of tasks performed by the admin, like adding or removing devices. Admin log.
- Links: List of all links in all maps.
- Logs: Logs of device statuses. Dude also includes a Syslog server, and can receive Logs from other devices.
- MIB nodes: Information about MIBs
- Network maps: All maps
- Networks: List of all network segments places on the map
- Notifications: Different ways to alert the admin of
- Panels: Allows to configure separate dude window entities for use on multiple monitors or otherwise
- Probes: Probes are responsible for polling specific services on the defices
- Services: Lists the currently monitored services on all devices
- Tools: Configures the tools that can be run on each device (ie. connect with winbox, telnet, ftp etc.)

How you should work with

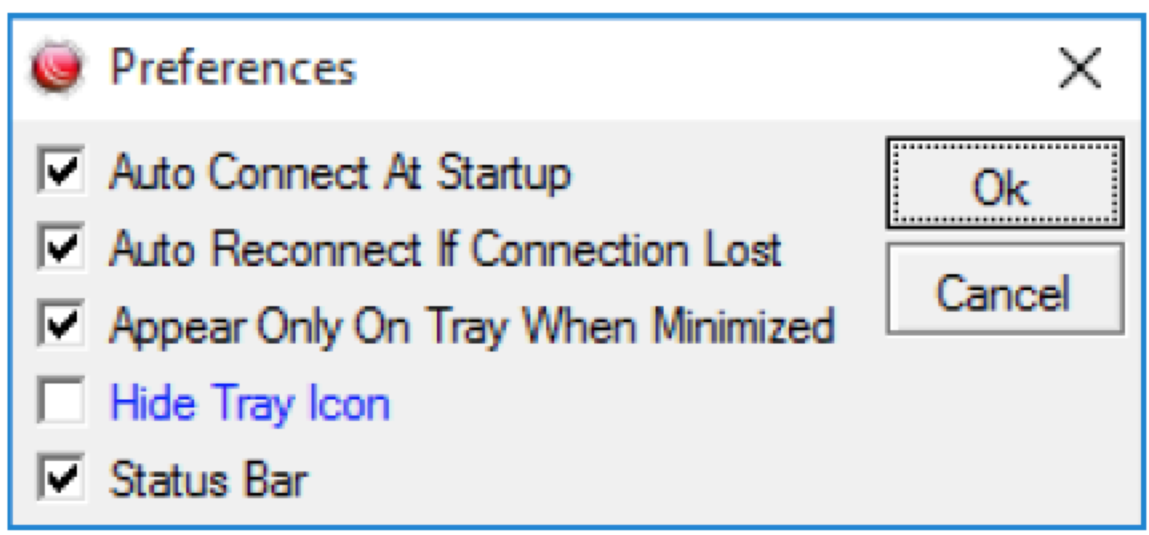
Server Settings





How you should work with

Preferences



Preferences

☑ Auto Connect At Startup

☑ Auto Reconnect If Connection Lost

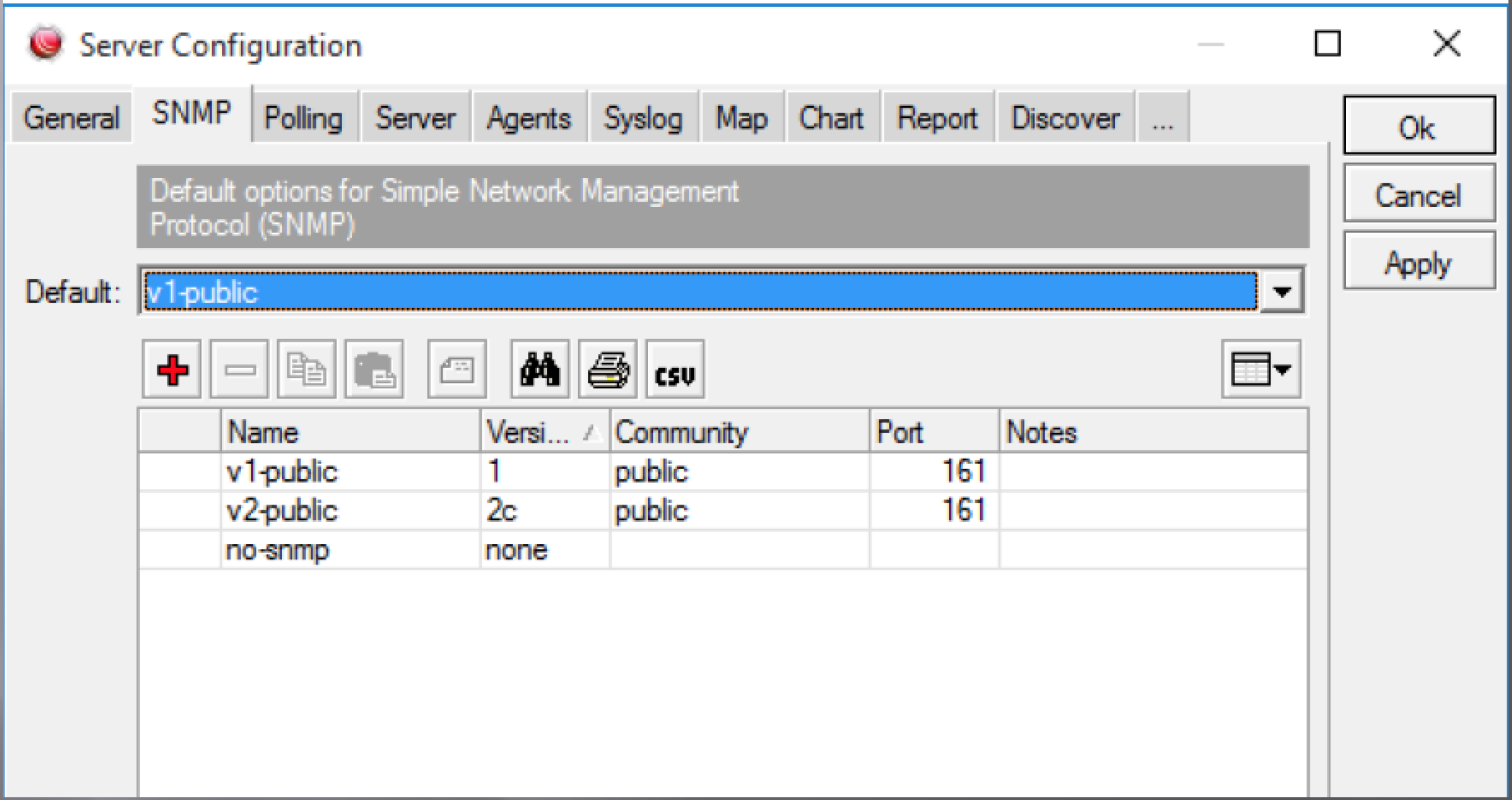
☑ Appear Only On Tray When Minimized

□ Hide Tray Icon

☑ Status Bar

How you should work with

Server Settings



Default options for Simple Network Management Protocol (SNMP)

Default: v1-public

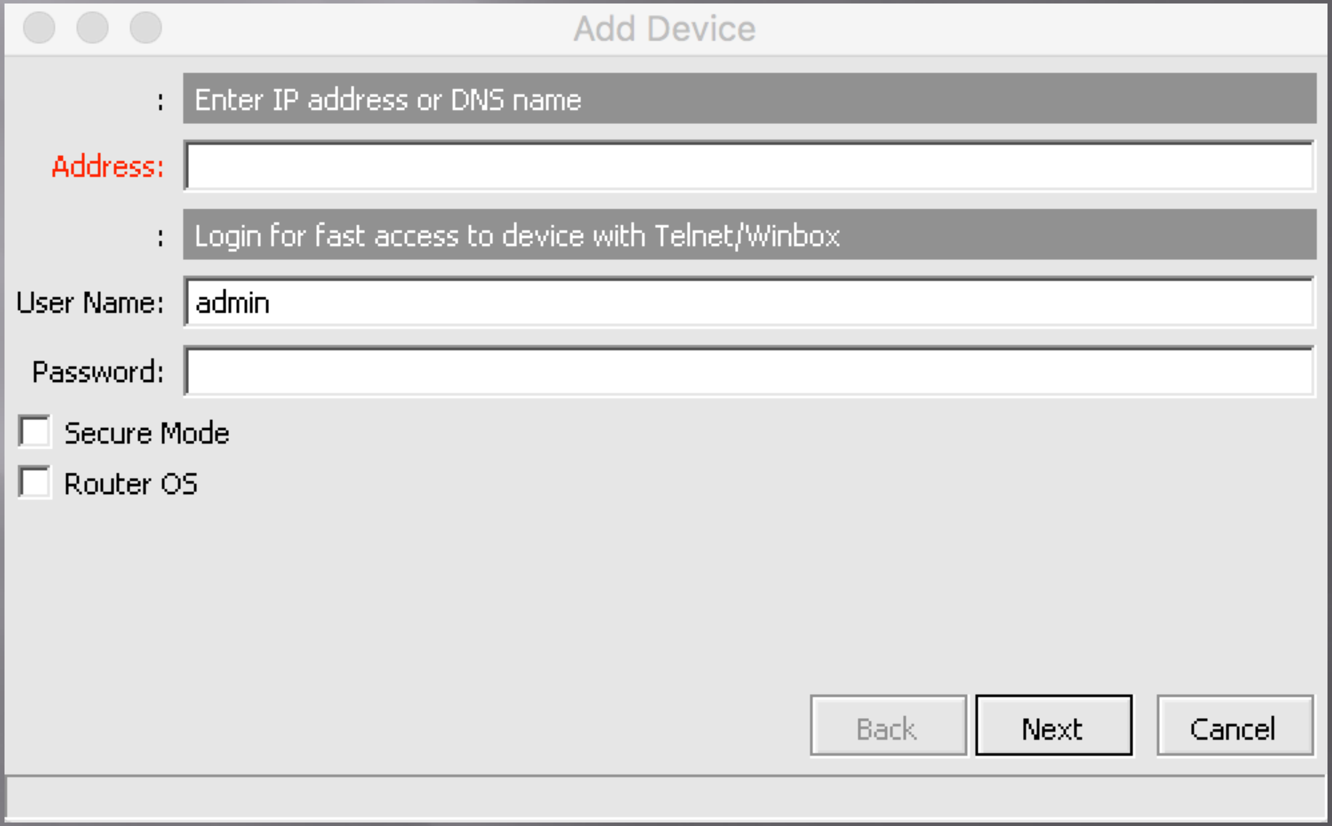
Name	Versi...	Community	Port	Notes
v1-public	1	public	161	
v2-public	2c	public	161	
no-snmp	none			

How you should work with

Device Settings

- Adding devices is just few steps:

1-



Add Device

: Enter IP address or DNS name

Address:

: Login for fast access to device with Telnet/Winbox

User Name: admin

Password:

☐ Secure Mode

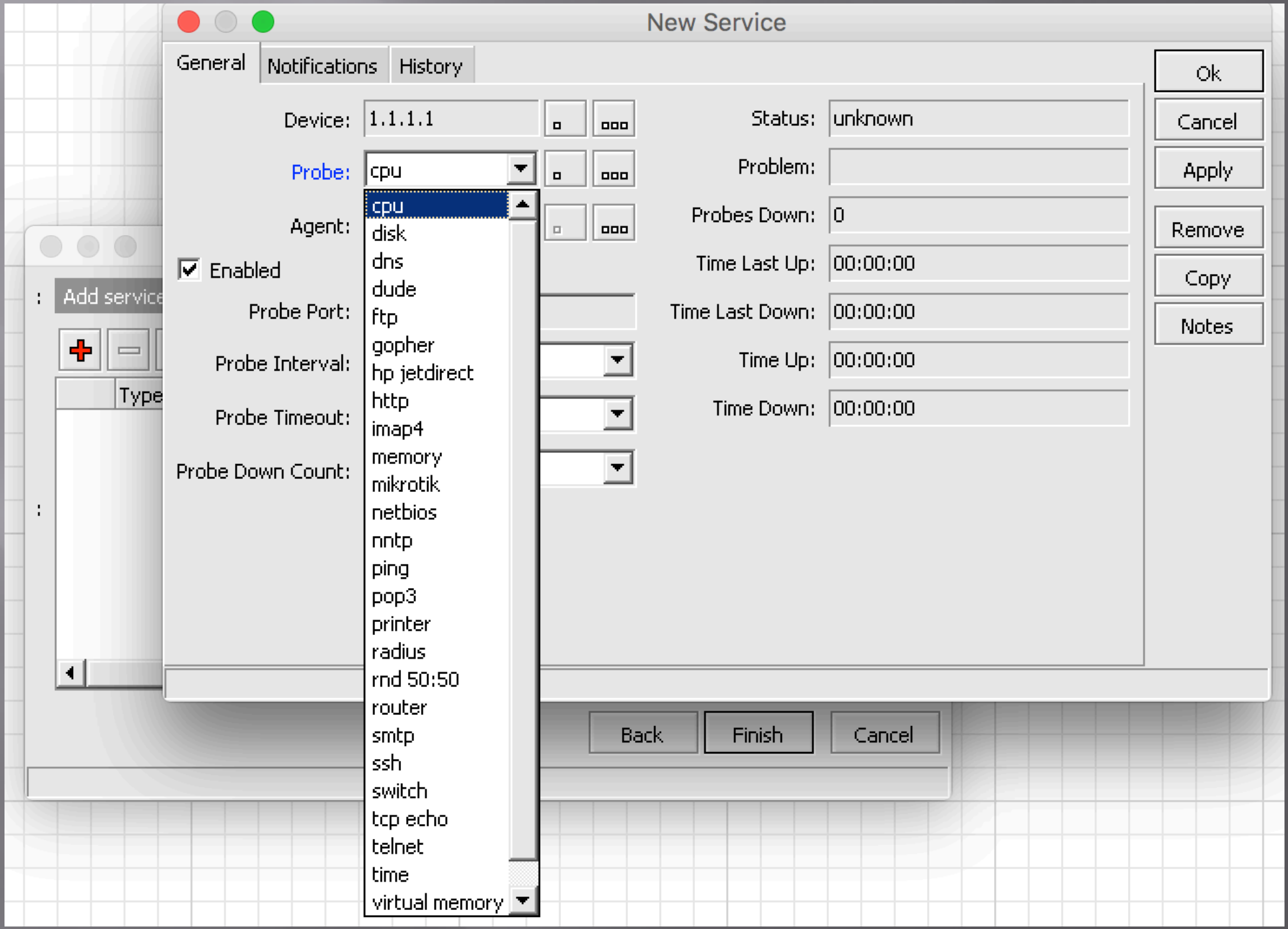
☐ Router OS

How you should work with

Device Settings

- Adding devices is just few steps:

2-



New Service

Device: 1.1.1.1

Probe: cpu

Agent:

☑ Enabled

Probe Port:

Probe Interval:

Probe Timeout:

Probe Down Count:

Status: unknown

Problem:

Probes Down: 0

Time Last Up: 00:00:00

Time Last Down: 00:00:00

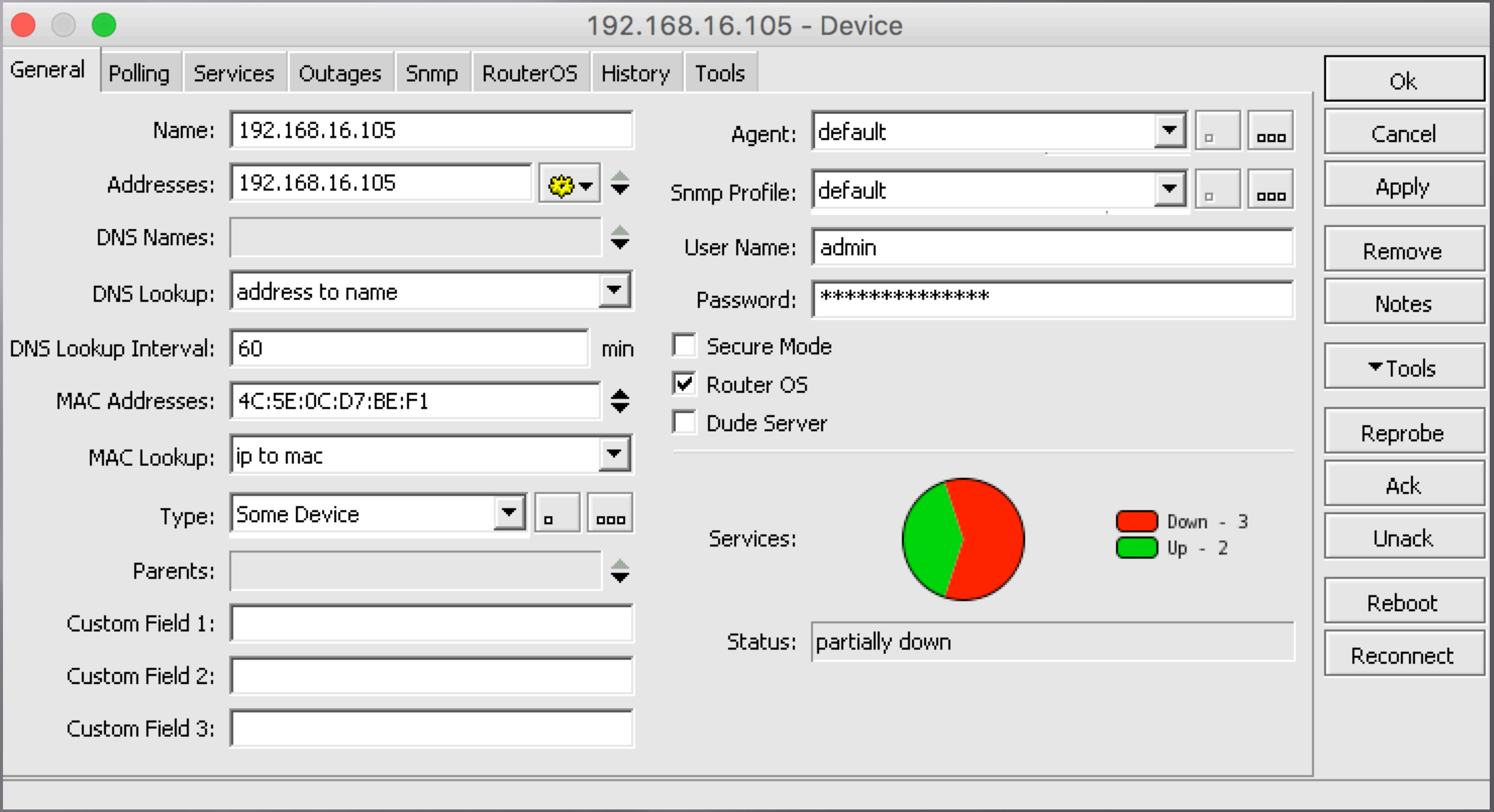
Time Up: 00:00:00

Time Down: 00:00:00

How you should work with

Device Settings

Important to configure accurate



192.168.16.105 - Device

Name:	192.168.16.105
Addresses:	192.168.16.105
DNS Names:	
DNS Lookup:	address to name
DNS Lookup Interval:	60 min
MAC Addresses:	4C:5E:0C:D7:BE:F1
MAC Lookup:	ip to mac
Type:	Some Device
Parents:	
Custom Field 1:	
Custom Field 2:	
Custom Field 3:	

Agent:	default
Snmp Profile:	default
User Name:	admin
Password:	**************

□ Secure Mode

☑ Router OS

□ Dude Server

Services: 🟥 Down - 3 🟩 Up - 2

Status: partially down

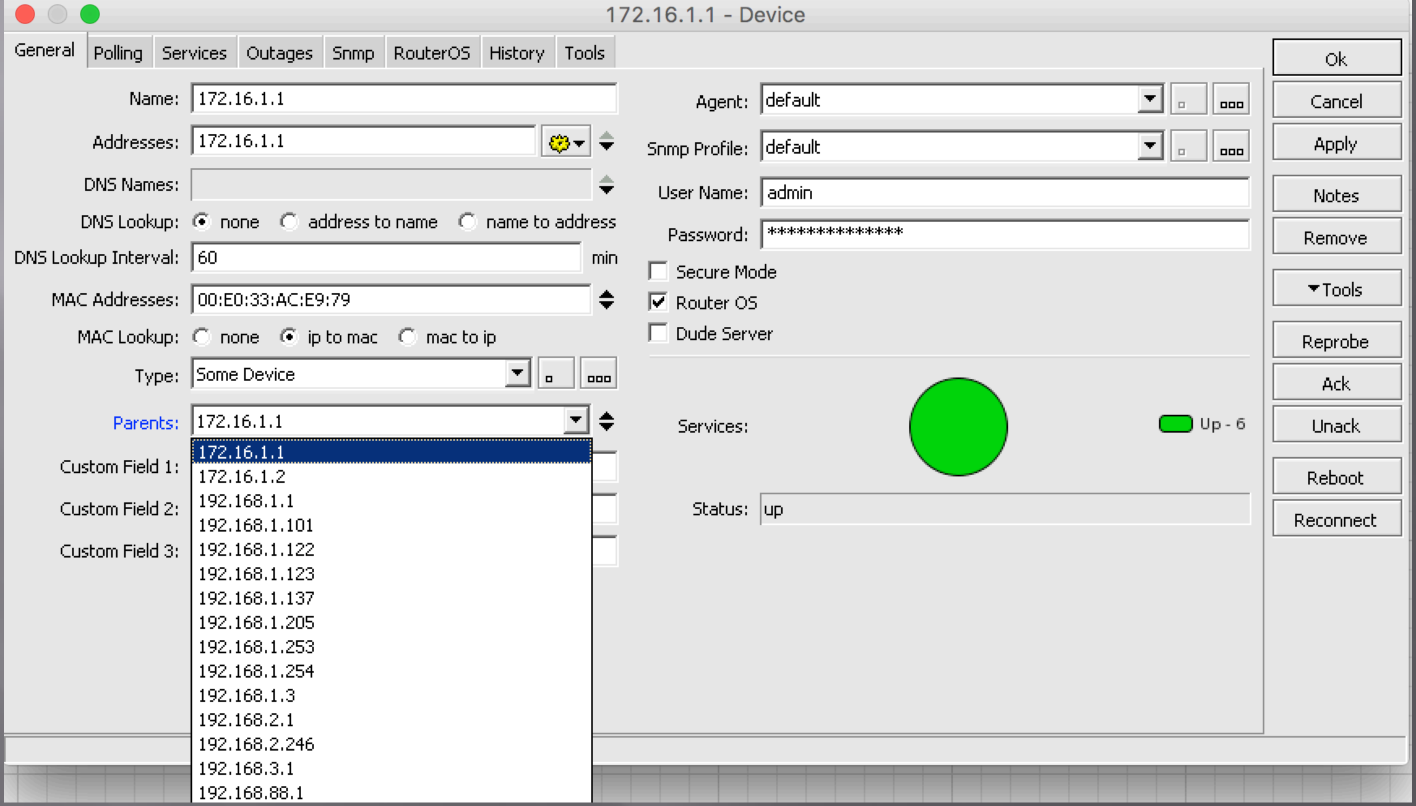
How you should work with Maps:

- Map Contains 2 Layers

1- Device links

2- Device dependencies

- To avoid receiving reports about each device status when a parent device is unreachable, you can make dependency between devices



Name: 172.16.1.1

Addresses: 172.16.1.1

DNS Names:

DNS Lookup: ● none ○ address to name ○ name to address

DNS Lookup Interval: 60 min

MAC Addresses: 00:E0:33:AC:E9:79

MAC Lookup: ○ none ● ip to mac ○ mac to ip

Type: Some Device

Parents: 172.16.1.1

- 172.16.1.1
- 172.16.1.2
- 192.168.1.1
- 192.168.1.101
- 192.168.1.122
- 192.168.1.123
- 192.168.1.137
- 192.168.1.205
- 192.168.1.253
- 192.168.1.254
- 192.168.1.3
- 192.168.2.1
- 192.168.2.246
- 192.168.3.1
- 192.168.88.1

Custom Field 1:

Custom Field 2:

Custom Field 3:

Agent: default

Snmp Profile: default

User Name: admin

Password: **************

☐ Secure Mode

☑ Router OS

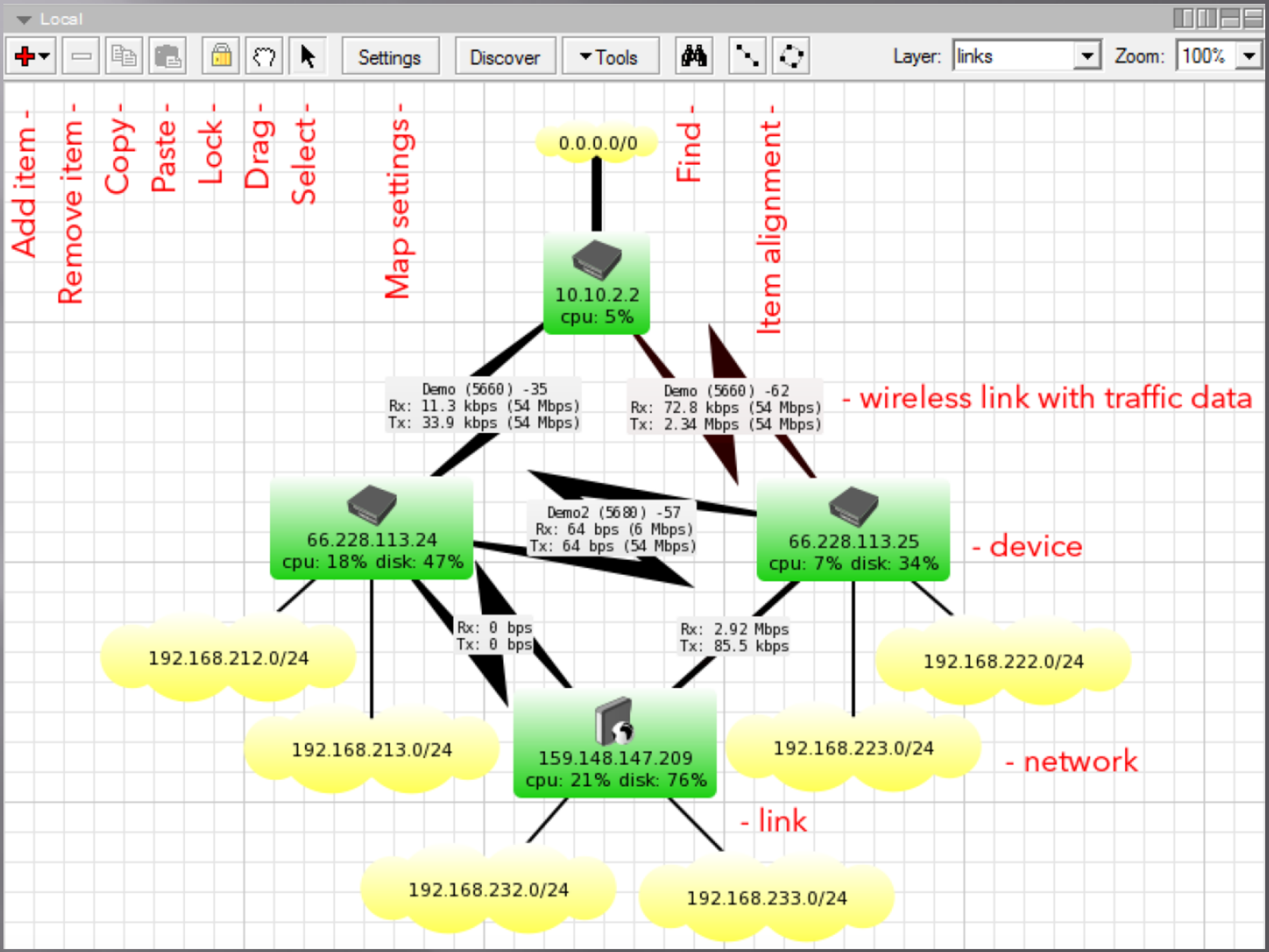
☐ Dude Server

Services: 🟩 Up - 6

Status: up

How you should work with

Maps:



Local

Settings | Discover | Tools

Layer: links

Zoom: 100%

Add item - Remove item - Copy - Paste - Lock - Drag - Select - Map settings - Find - Item alignment -

- wireless link with traffic data

- device

- network

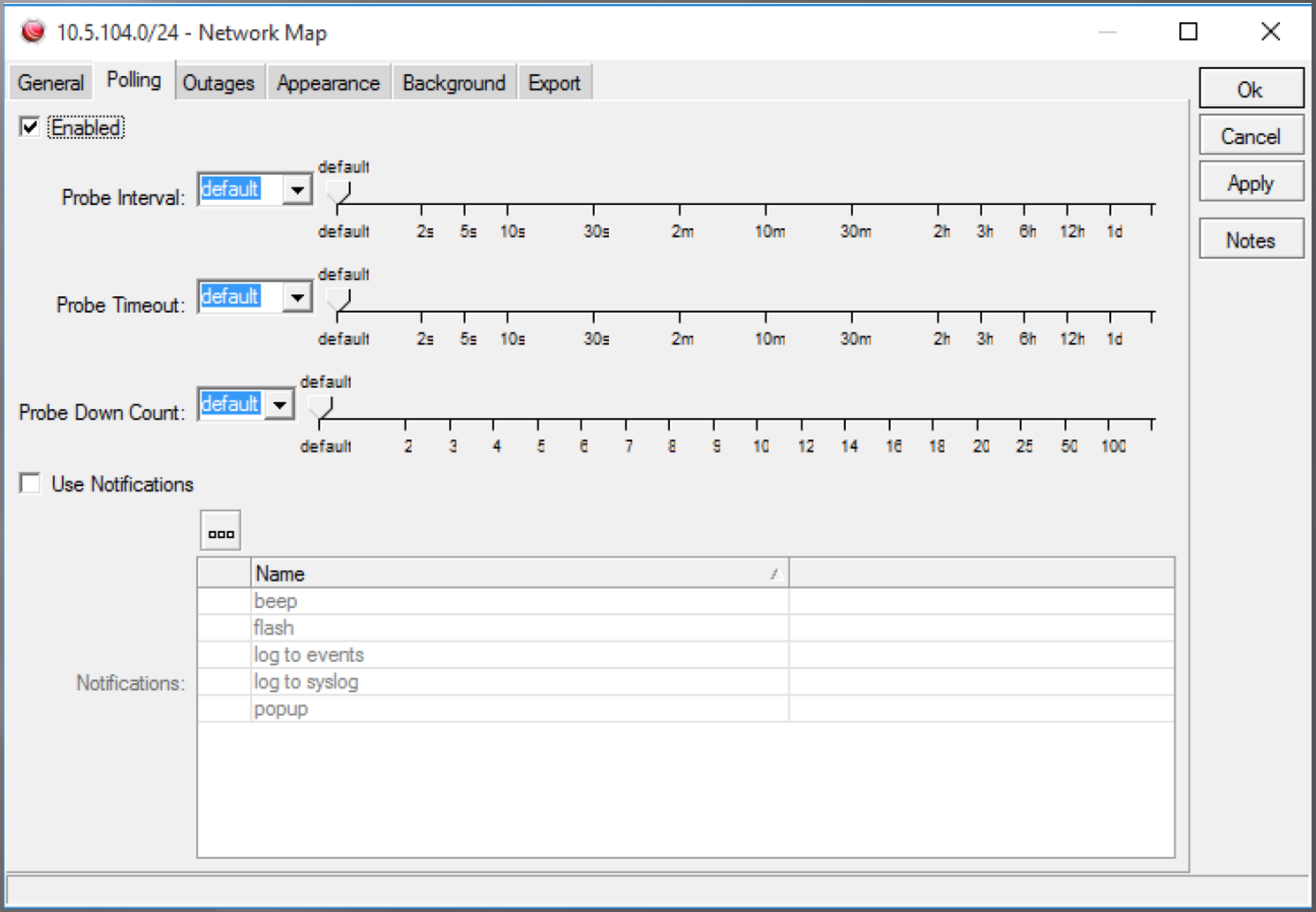
- link

How you should work with

Maps:

- Polling: This tab allows you to configure polling times and timeouts specifically for this map.

Map specific settings are always overriding general settings, but device specific settings take preference.



10.5.104.0/24 - Network Map

☑ Enabled

Probe Interval: default

Probe Timeout: default

Probe Down Count: default

□ Use Notifications

Notifications:

	Name
	beep
	flash
	log to events
	log to syslog
	popup

General
Polling
Outages
Appearance
Background
Export
Ok
Cancel
Apply
Notes
default
default 2s 5s 10s 30s 2m 10m 30m 2h 3h 6h 12h 1d
default
default 2s 5s 10s 30s 2m 10m 30m 2h 3h 6h 12h 1d
default
default 2 3 4 5 6 7 8 9 10 12 14 16 18 20 25 50 100
...

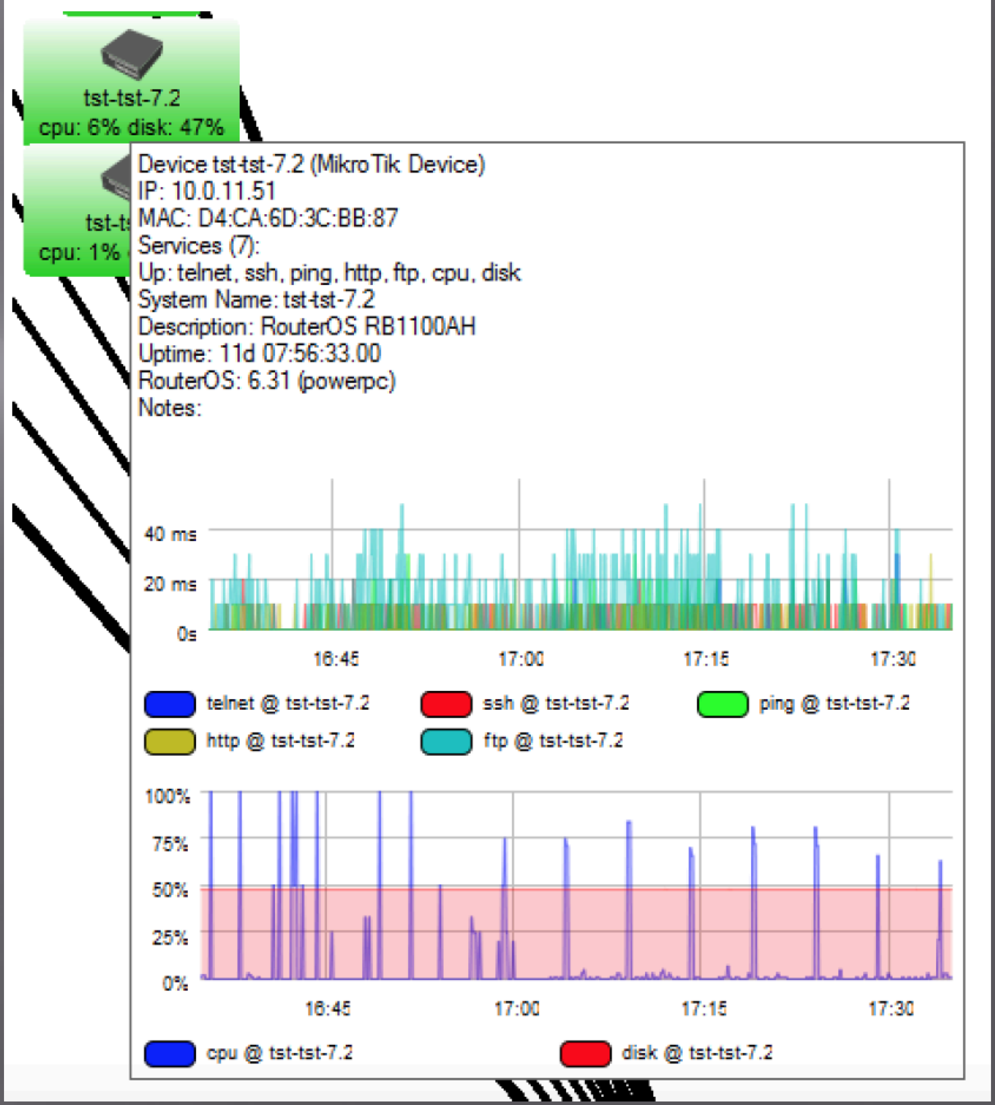
How you should work with

By The Way!!!!!!!

- You also can monitor and have a graph of real time device's traffic

Interesting!!! Isn't it????

:) :) :) :)

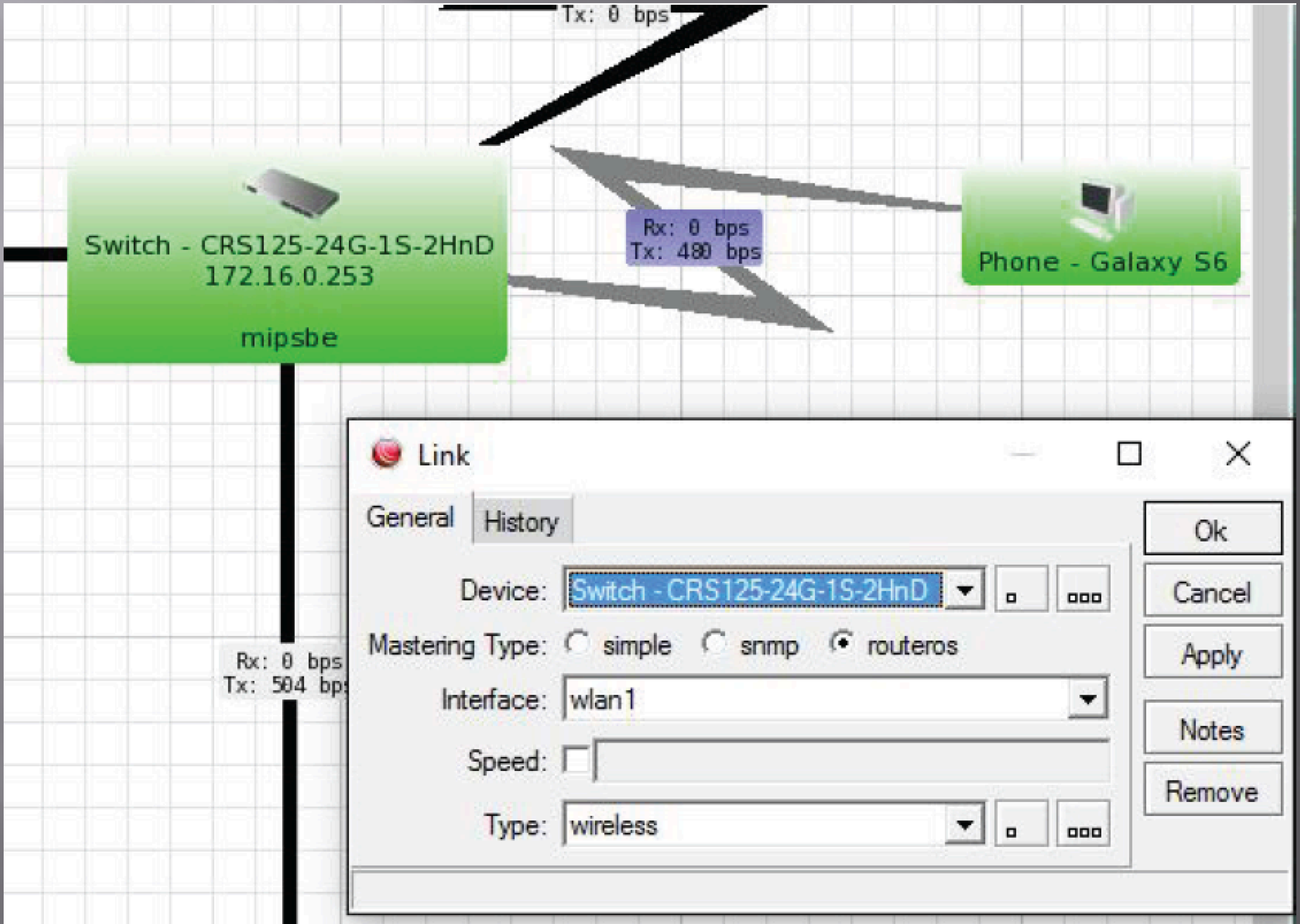


Device tst-tst-7.2 (MikroTik Device)
IP: 10.0.11.51
MAC: D4:CA:6D:3C:BB:87
Services (7):
Up: telnet, ssh, ping, http, ftp, cpu, disk
System Name: tst-tst-7.2
Description: RouterOS RB1100AH
Uptime: 11d 07:56:33.00
RouterOS: 6.31 (powerpc)
Notes:

How you should work with

Links

- Links list, shows all your links (different types)
- Also you can add links directly from the Map



Device: Switch - CRS125-24G-1S-2HnD

Mastering Type: ○ simple ○ snmp ● routeros

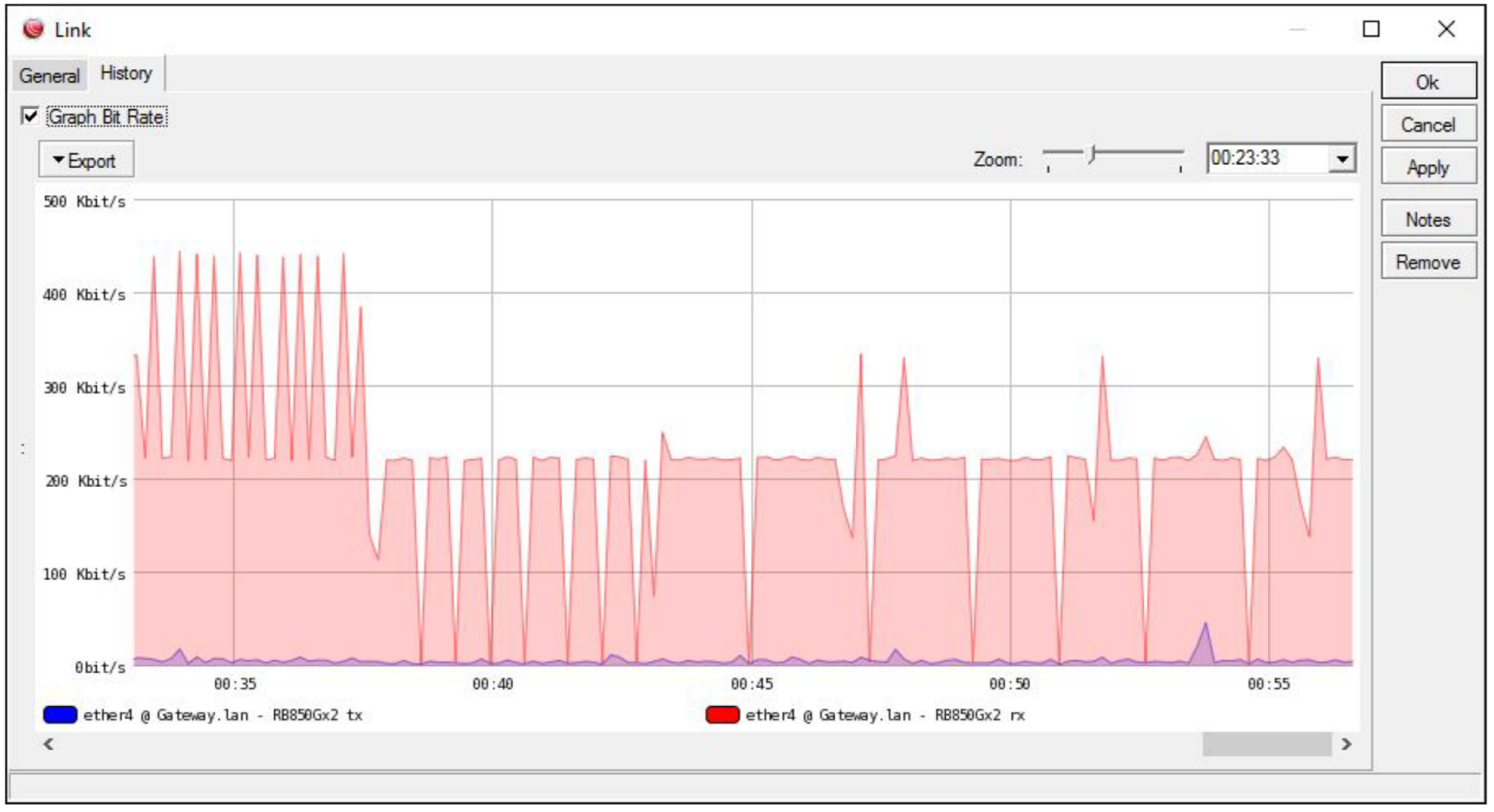
Interface: wlan1

Speed: □

Type: wireless

How you should work with Links

- By checking out link history, you can find out graphs



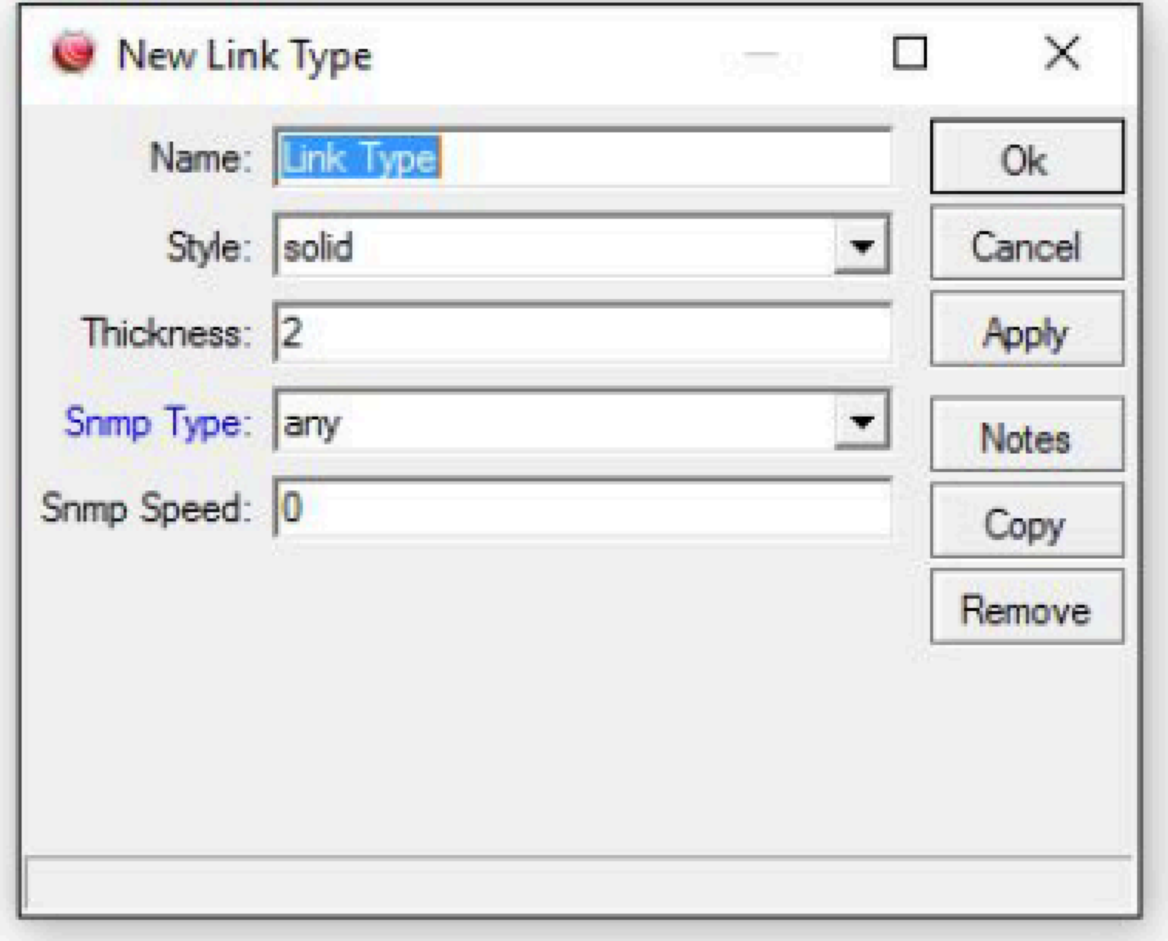
☑ Graph Bit Rate

Zoom: 00:23:33

How you should work with

Links

- There are some Link types by default, but also you can add your own type



New Link Type

Name: Link Type

Style: solid

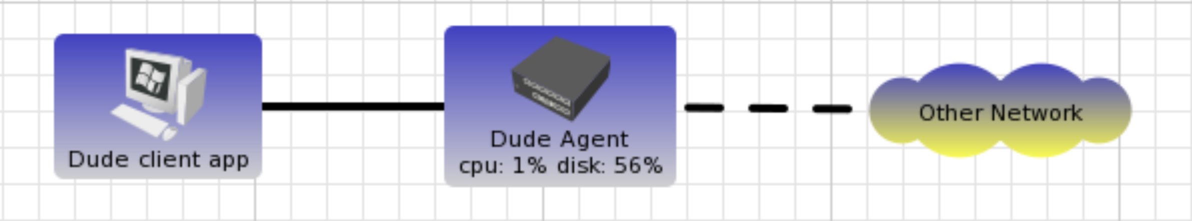
Thickness: 2

Snmp Type: any

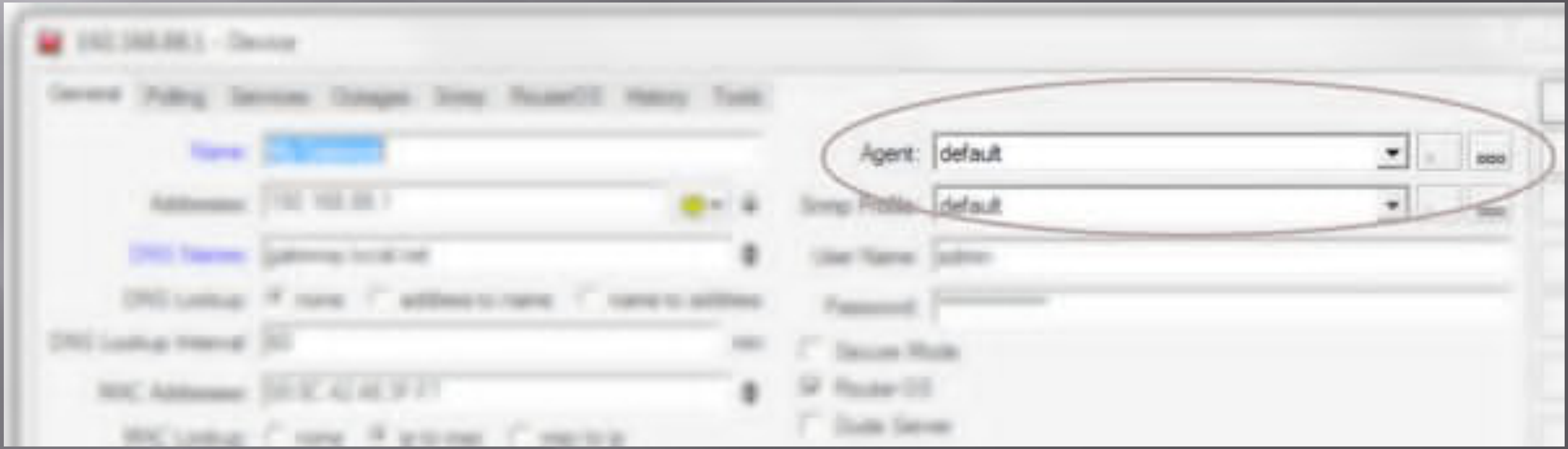
Snmp Speed: 0

Monitoring

Agents



Agents are other Dude servers that can be used as intermediaries for dev monitoring.



192.168.88.1 - Device

General | Polling | Services | Outages | Snmp | RouterOS | History | Tools

Name: [illegible]

Addresses: 192.168.88.1

DNS Names: gateway.local.net

DNS Lookup: ● name ○ address to name ○ name to address

DNS Lookup Interval: 60

MAC Addresses: [illegible]

MAC Lookup: ○ none ● ip to mac ○ mac to ip

Agent: default

Snmp Profile: default

User Name: admin

Password:

□ Secure Mode

☑ RouterOS

□ Dude Server

Monitoring

Notifications:

- It's possible to configure any actions that can be taken when a device status changes.

The predefined Notifications are the following:

1-Beep: Makes a beeping from the PC speaker of the server

2-Flash: Flashes the Dude taskbar menu

3-Log to Events: Saves information to local Event log

4-Log to Syslog: Saves information to Syslog

5-Popup: Opens a small notification window

Monitoring

Notifications:

You can also add new Notifications, more types are available

1-Email: Sends email, need to specify Server address

2-Execute locally: Run command on the local Windows machine (where Dude viewer runs), can pass variables

3-Sound: Plays sound. Sound files can be uploaded and chosen here

4-Group:Executes a group of actions

5-Speak: Uses Windows speech ability to say the message in a computerized voice

6-Log: Saves to local Dude Log file

7-Syslog: Saves to remote Syslog server. Need to specify Syslog address

But Something missing here!!!!!!!

GSM Notification:

Sending text message to notify!!!!!!

What??????????

Now, let’s talk about

iGenTik

Order Notification SMS
Swisscom
16:57
Messages
+1 (769) 553-5...
Edit
Call
Add to Contacts
Text Message

iGenTik

- iGenTik is Interactive GSM/Email notification system,

Based on MikroTik platform

with customizable GUI Interface

To notify **anything you imagine**

iGenTik

- built-in battery that can be alive for around an hour
- Sending notification by Text Message or Email about all Device's activities in the Network including:
  1. Any Public or Private host reachability
  2. VPN Connections: as soon as any VPN connections get connected,
  3. Queuing: if one queue rule gets 50%, 75% or 100% bandwidth
  4. by adding any route (Static, Dynamic) in routing table
  5. main/failover upstream replacement
  6. check ISP gateway: to make sure the availability of providers
  7. Firewall/NAT/Mangle Control: by adding any rules in these tables
  8. Logs notifications
  9. Traffic Control: weird TX/RX bandwidth
  10. Protocol check: weird UDP/TCP.ICMP… traffic
  11. Any kind of attack:

      I. IP/Port Scan
      II. DDOS Attack
      III. Phishing Attack
      IV. Hijack Attack
      V. Buffer Attack
      VI. Password Attack
      VII. IP Spoofing
      VIII. Sniffing
      IX. Application Layer Attack

iGenTik

12. Wireless Control:
    I. providing wrong pass by clients for several times
    II. registration table reports (list of connected clients)
    III. unwanted wireless login
13. City/UPS Power Check
    I. voltage balance
    II. Ampere balance
    III. City Power up/down
    IV. UPS power up/down
14. Elastix (Any VOIP Call Center) logs and reports including:
    I. Emergency Calls
    II. Call Duration
    III. Trunk Failure
    IV. Call Center Failure
    V. Operator timeout
15. Antivirus Management notification (Kaspersky, Node, …)

iGenTik

The Most interesting default features

- Replying Text Messages by receiving any Text Message (means you can send commands to it by messages or emails to get reports or to push doing something) including:

- Sending remote commands to get reports and logs

- Sending remote commands to any other device in the Network for
  I. Disable/Enable Interface
  II. Block/Unblock Users
  III. Allow/Terminate any connections
  IV. Turn on/turn off or restart Servers, routers …

iGenTik

Has not released yet

Will announced as MikroTik MfM Project in a month

And will be ready to use sooooooooon….

ANY
questions?

Contact Details

Turk Cell:	+90 (537) 495 3233
Persian Cell:	+98 (912) 149 7009
International Cell:	+37259431151
Skype:	mani_raissdana

m.raissdana@mits-co.com

raissdana.mani@gmail.com

www.mits-co.com

YouTube

MikroTikEngineers

mani_raissdana

mikrotikiran

@mani_raissdana

Mani Raissdana

Good Luck

&

Enjoy MUM